DURIE TANGRI LLP
Daralyn J. Durie (SBN 169825)
ddurie@durietangri.com
217 Leidesdorff Street
San Francisco, California,94111
+1 (415) 362-6666
+1 (415) 236-6300 facsimile

Attorney for Defendant Orange, S.A.

FOLEY HOAG LLP
Daniel Schimmel (*pro hac vice)*
dschimmel@foleyhoag.com
1540 Broadway, 23rd Floor
New York, New York, 10036
+1 (646) 927-5500
+1 (646) 927-5599 facsimile

Anthony Mirenda (*pro hac vice*)
amirenda@foleyhoag.com
Seaport West
155 Seaport Boulevard
Boston, MA 02210
+1 (617) 832-1220
+1 (617) 832-7000 facsimile

Attorneys for Defendants

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

TELESOCIAL, INC.,

Plaintiff,

v.

ORANGE S.A., et al.,

Defendants.

Case No. 3:14-cv-03985-JD

DEFENDANTS' TRIAL BRIEF

Judge: Honorable James Donato
Trial: April 10, 2017

I. INTRODUCTION

Telesocial initiated this case in 2014, seeking to recover on several state law claims and the Computer Fraud and Abuse Act ("CFAA"). Telesocial's case is based on its theory that Orange and eleven current and former employees and interns (collectively, the "Orange Defendants") hacked into Telesocial's servers and fraudulently copied its "crown-jewel software code" for Telesocial's Call Friends application and used it to develop and launch Orange's own social calling product, Party Call. Dkt. 1. In denying the Orange Defendants' motion to dismiss on *forum non conveniens* grounds, the Court credited Telesocial's representations about its theory and proof, and permitted this case to proceed to discovery. Dkt. 85 ("As the facts alleged in the FAC make clear, this claim is premised entirely upon events that occurred after the abrupt termination of the discussions subject to the NDA, and is necessarily based on Orange's unauthorized access to information that Telesocial did not disclose during those negotiations."). [1] Telesocial has now had the opportunity to engage in extensive discovery to find some factual support for its "hacking" and related trade secrets claims. It has come up empty handed.

In light of the legal deficiencies and lack of any evidentiary support for Telesocial's claims, the Orange Defendants have filed a motion for summary judgment on all counts. The Orange Defendants have also filed motions under *Daubert* to exclude the testimony and opinions of both of Telesocial's damages experts and a motion to exclude the testimony and opinions of its code expert. Those motions remain pending, as so this Trial Brief will address all of Telesocial's causes of action (which, for many, involve multiple liability theories) and the related affirmative defenses. Specifically:

- Telesocial's causes of action for "hacking" under the Computer Fraud and Abuse Act ("CFAA") and California Computer Data Access and Fraud Act ("CDAFA").

[1] The Court's denial of the Orange Defendants' motion to dismiss for *forum non conveniens* does not bear on the issues to be addressed in this Trial Brief – that is, the claims remaining be tried and the applicable legal standards – and so the Court's decision is not further addressed in this Trial Brief. In any event, the Orange Defendants have already presented detailed legal arguments on this issue at the motion to dismiss stage and, therefore, this issue is adequately preserved for appeal. *See, e.g.*, *Mukhtar v. Cal. State Univ.*, 299 F.3d 1053, 1063 (9th Cir. 2002), *overruled on other grounds by Estate of Barabin v. AstenJohnson, Inc.*, 740 F.3d 457 (9th Cir. 2014).

- Telesocial's cause of action under the California Uniform Trade Secrets Act ("CUTSA").
- Orange's affirmative defense to Telesocial's CUTSA claim that the purported "trade secrets" were readily ascertainable.
- Telesocial's cause of action under the California Unfair Competition Law ("UCL").
- Orange's affirmative defense to Telesocial's UCL claim that it is preempted by CUTSA.
- Telesocial's breach of contract causes of action.
- Orange's affirmative defense that Telesocial failed to use reasonable efforts to mitigate its damages.

Except for Telesocial's claim for punitive damages under the CDAFA and CUTSA, each of the foregoing issues are to be tried under a preponderance of the evidence standard. As to the punitive damages claim, Telesocial must prove by clear and convincing evidence that each defendant engaged with fraud, oppression or malice.

All of Telesocial's claims fail because of an absence of proof as to one or more essential elements of each claim as to each defendant and submitting this case to the jury invites a judgment based upon speculation. At the conclusion of the case, if Orange prevails, the Court will also need to decide, in light of the exceptional nature of this case, whether each of the defendants are entitled to its costs, expenses, and reasonable attorneys' fees.

II. CAUSES OF ACTION AND AFFIRMATIVE DEFENSES FOR JURY TRIAL

Pursuant the Court's Standing Order, Orange specifies below each cause of action and affirmative defense remaining to be tried, along with a statement of the applicable legal standard.

a. Telesocial's CFAA Claim.

It is well-established that the CFAA is a criminal anti-"hacking" statute, not a misappropriation statute and it requires evidence of unauthorized *access* by the defendant to a protected computer system. *See United States v. Nosal*, 676 F.3d 854, 857-59 (9th Cir. 2012) (*"Nosal I"*). Absent evidence of access to a protected computer, neither misappropriation nor use of a computer system "contrary to the [owner's] interests" is sufficient to create liability. *LVRC*

Holdings LLC v. Brekka, 581 F.3d 1127, 1130-31 (9th Cir. 2009). Telesocial claims that each Orange defendant violated four different provisions of the CFAA: 18 U.S.C. §§ 1030(a)(2)(c), 1030(a)(4), 1030(a)(5), and 1030(a)(6). Each statutory provision at issue has distinct essential elements, and Telesocial must prove each essential element as to each individual defendant and corporate defendant by a preponderance of the evidence.

First, to prevail on its claim that each Orange defendant violated Section 1030(a)(2)(c), Telesocial must prove each of the following elements as to each defendant: (1) each defendant intentionally accessed a protected Telesocial computer "without authorization" or "exceeded authorized access" to a protected Telesocial computer; (2) by accessing that protected computer, each defendant obtained information from a computer that was used in or affected commerce or communication between one state and another state, or between a state of the United States and a foreign country; and (3) each defendant's actions resulted in at least $5,000 in losses to Telesocial.

Under the CFAA, "a person uses a computer 'without authorization' when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." *Brekka*, 581 F.3d at 1135. Use of a computer contrary to the owner's interest does not alone satisfy the "without authorization" prong of the statute. *Id.* In addition, "exceeds [or exceeded] authorized access" limits the applicability of the CFAA to violations of restrictions on access to information, and not restrictions on the use of information that is permissibly accessed. *Nosal I*, 676 F.3d at 864; *see also United States v. Christensen*, 828 F.3d 763, 787 (9th Cir. 2015), *as amended on denial of reh'g* (July 8, 2016). In other words, Telesocial's CFAA claim cannot rely on a breach of a contractual Terms of Use to establish unauthorized access. *Nosal I*, 676 F.3d at 860-62; *Facebook, Inc. v. Power Ventures. Inc.*, 828 F.3d 1068, 1078 (9th Cir. 2016) ("[A] violation of the terms of use of a website cannot itself constitute access without authorization."). Even misuse of a "password" does not satisfy the "exceeds authorized access" prong if the defendant had permission to access the computer system in the first instance. *Nosal I*, 676 F.3d at 864.

Second, as to Section1030(a)(4), Telesocial must prove as to each defendant that: (1) each defendant "knowingly" accessed "without authorization" or "exceeded authorized access" to a protected Telesocial computer used in or affecting interstate or foreign commerce or communication; (2) each defendant did so with "the intent to defraud"; (3) by accessing the protected computer "without authorization" or in "excess of authorized access," each defendant furthered the intended fraud; (4) by accessing the protected computer "without authorization" or in "excess of authorized access," each defendant obtained something of value; and (5) the total value of defendant's computer use exceeded $5,000 between August 2012 and December 2012. A defendant does not have an "intent to defraud" if he or she acted in good faith and without an intent to deceive or cheat. *See United States v. Shipsey*, 363 F.3d 962, 967-68 (9th Cir.), *cert. denied*, 543 U.S. 1004 (2004); *United States v. Molinaro*, 11 F.3d 853, 863 (9th Cir. 1993).

Third, to Section 1030(a)(5), Telesocial must prove as to each defendant that: (1) each defendant intentionally accessed a protected Telesocial computer "without authorization;" (2) the computer was used in or affected interstate or foreign commerce or communication; (3) as a result of each defendant's access, each defendant caused the impairment to the integrity or availability of Telesocial's data, system, information, or programs; and (4) each of the defendant's actions caused a loss to Telesocial of at least $5,000.

Finally, Telesocial also claims that each Orange Defendant violated Section 1030(b) by unlawfully conspiring to obtain information from a protected computer system. To prove a conspiracy under 18 U.S.C. § 371, Telesocial must establish: "(1) an agreement to engage in criminal activity, (2) one or more overt acts taken to implement the agreement, and (3) the requisite intent to commit the substantive crime." *United States v. Kaplan*, 836 F.3d 1199, 1212 (9th Cir. 2016) (citation and internal quotation marks omitted).

b. Telesocial's CDAFA Claim.

Like the CFAA, the CDAFA also targets "hacking." *See, e.g.*, *Christensen*, 828 F.3d at 789. Telesocial claims that the Orange Defendants violated four separate provisions of the CDAFA: Cal. Pen. Code §§ 502(c)(1), 502(c)(2), 501(c)(6), and 501(c)(7). First, to prevail on its

claim that each defendant violated Section 502(c)(1), Telesocial must prove that: (1) each defendant "knowingly accessed and without permission" used a protected Telesocial computer, computer system, or computer network; (2) each defendant did so in order to execute a scheme to defraud, or to wrongfully obtain property or data, and (3) each defendant's actions caused damage or loss to Telesocial. Like the CFAA, a defendant does not violate the CDAFA if it had "permission" to access the system in the first instance and that permission was never expressly revoked. *Power Ventures*, 828 F.3d at 1079. In addition, Telesocial cannot meets its evidentiary burden by relying on a purported breach of Terms of Use, unless each defendant was informed of the breach, requested to cease the conduct, and continued notwithstanding the demand to cease. *See, e.g., Power Ventures*, 828 F.3d at 1079.

Second, as to Section 502(c)(2), Telesocial must prove that: (1) each defendant "knowingly accessed and without permission" took, copied, or made use of any data from a protected Telesocial computer, computer system, or computer network; and (2) each defendants' actions caused damage or loss to Telesocial.

Third, as to Section 502(c)(6), Telesocial must prove that: (1) each defendant "knowingly accessed and without permission" provided or assisted in providing a means of accessing a protected Telesocial computer, computer system, or computer network; and (2) each defendant's actions caused damage or loss to Telesocial.

Fourth, as to Section 502(c)(7) of the CDAFA, Telesocial must prove by a preponderance of the evidence that: (1) each Orange Defendant "knowingly accessed and without permission" accessed or caused to be accessed a protected Telesocial computer, computer system, or computer network; and (2) each defendant's actions caused damage or loss to Telesocial.

Finally, Telesocial alleges that the Orange Defendants conspired to violate the CDAFA, which requires Telesocial to prove as to each defendant that: (1) the defendant was aware that one or more of the co-conspirators planned to violated the CDAFA, and (2) the defendant agreed with one or more of the co-conspirators and intended that the violated be committed.

c. Telesocial's California Uniform Trade Secrets Act ("CUTSA") Claim.

Telesocial has claimed that Orange has misappropriated six purported trade secrets. To prevail, Telesocial must establish for each of its six claimed trade secrets that: (1) Telesocial owned the claimed trade secret information; (2) that it was a "secret" at the time of the purported misappropriation (that is, the information was a secret, the information had economic value because it was a secret, and Telesocial made "reasonable efforts" to keep the information a secret); (3) that Orange misappropriated the "trade secrets" through improper means; (4) that Telesocial was harmed, or Orange was unjustly enriched, by the misappropriation of the trade secret; and (5) that the improper acquisition, use, or disclosure was a substantial factor in causing the harm. *See* Cal. Civ. Code, § 3426.1 *et seq.* As to the "improper" means requirement, Telesocial must prove that each Orange defendant engaged in some type of improper conduct, like hacking or electronic eavesdropping or espionage, to obtain the information. *See* Cal. Civ. Code, § 3426.1(a). CUTSA expressly provides that "reverse engineering" is not improper, nor is observing information that is publicly available on the internet, nor is engaged in independent efforts to invent or discovery the information. *Id.*

d. Orange's Affirmative Defense to Telesocial's CUTSA claim.

As to the affirmative defense for which Orange will bear the burden of proof, Orange intends to prove at trial its affirmative defense that the "trade secrets" were "readily available." Telesocial's so-called "trade secrets" were not "secrets" because they are either readily ascertainable in the public domain or they had been disclosed publicly without protection. To prevail on this affirmative defense, Orange has the burden of proving by a preponderance of the evidence that each purported "trade secret" was readily ascertainable by proper means at the time of the alleged misappropriation. There is no "fixed standard" for determining what is "readily ascertainable by proper means." In general, information is readily ascertainable if it can be obtained, discovered, developed, or compiled without significant difficulty, effort, or expense. *See San Jose Constr. v. S.B.C.C., Inc.*, 155 Cal. App. 4th 1528, 1542-43 (Cal. App. Ct. 2007). Here, Orange will prove by a preponderance of the evidence that all six of Telesocial's purported "trade

secrets" were publicly available and ascertainable through the normal use of the publicly available Call Friends application. To the extent Orange carries its burden on this affirmative defense on each of Telesocial's so-called "trade secrets," the Orange Defendants will be entitled to a judgment in their favor.

e. Telesocial's UCL Claim.

Telesocial claims that the Orange Defendants violated the California Unfair Competition law by engaging in "unlawful" or "unfair" "business practices." For the purposes of the UCL, a practice that violates state or federal law may be an "unlawful" business practice. Telesocial claims that each Orange defendant is liable under the UCL because each Orange Defendant violated the CFAA and/or the CDAFA. Cal. Bus. & Prof. Code § 17200.

f. Orange's Affirmative Defense to Telesocial's UCL Claim.

No Orange defendant is liable under the UCL because that claim is preempted by CUTSA. UCL claims are preempted by CUTSA if they are predicated on the same facts as a claim for misappropriation of trade secrets. *See Digital Envoy, Inc. v. Google, Inc.*, 370 F. Supp. 2d 1025, 1034-35 (N.D. Cal. 2005). The preemption determination turns on whether the UCL claim is based on the same nucleus of facts as the trade secrets misappropriation claim. *K.C. Multimedia, Inc. v. Bank of Am. Tech. & Operations, Inc.*, 171 Cal. App. 4th 939, 961-62 (Cal. App. Ct. 2009). The evidence presented at trial will show that Telesocial's UCL claim is based entirely on the same nucleus of operative facts as its trade secrets claim.

g. Telesocial's Breach of Contract Claim.

Telesocial claims that the Orange Defendants are liable for breach of contract based on a violation of three provisions of a Terms of Use. To prevail on its contract claim, Telesocial must first prove that the ToU, which by its terms applied to Telesocial's API (as opposed to its Call Friends application), formed a binding contract with each of the Orange Defendants and governed their use of Call Friends. To satisfy this burden, Telesocial must prove that: (1) it and each Orange defendant entered into a contract, (2) that the contract terms were clear enough that the parties could understand what each was required to do, (3) that the parties agreed to give each other

something of value, and (4) that the parties agreed to the terms of the contract. Because the ToU is a "browsewrap" agreement and no defendant actually read the ToU, Telesocial must also put forward sufficient facts to establish that each defendant had "constructive notice" of its terms. *Nguyen v. Barnes & Noble, Inc.*, 763 F.3d 1171 (9th Cir. 2014); *In re Facebook Biometric Info. Privacy Litig.*, No. 15-cv-03747, 2016 U.S. Dist. LEXIS 60046 (N.D. Cal. May 5, 2016). To the extent Telesocial establishes the existence of a contract between it and any Orange defendant, it must then prove the elements of a breach of contract claim. In relevant part, this will require evidence that each Orange defendant did something that the contract prohibited it from doing (i.e., reverse engineered the API, used the API for a competitive purpose, or used the API in an unlawful way), and that Telesocial suffered damages as a result.

h. Telesocial's Breach of the Implied Covenant of Good Faith and Fair Dealing Claim.

Telesocial claims that the Orange Defendants are liable for breach of the implied covenant of good faith a fair dealing. To prove a breach of the implied covenant of good faith and fair dealing, Telesocial must prove the following elements: (1) the Telesocial and each Orange Defendant entered into a contract; (2) Telesocial did all, or substantially all, of the significant things that the contract required it to do; (3) that each Orange Defendant unfairly interfered with Telesocial's right to receive the benefits of the contract; and (4) that Telesocial was harmed as a result. *See generally Careau & Co. v. Sec. Pacific. Bus. Credit, Inc.*, 222 Cal App. 3d 1371, 1395 (1990). Telesocial cannot recover for a breach of the implied covenant of good faith and fair dealing if it is based on nothing more than the same facts supporting its breach of contract claim, including the same measure of damages, and so it may be disregarded as superfluous. *Id.*

i. Orange's Affirmative Defense that Telesocial Failed to Mitigate its Damages.

Orange claims that Telesocial is not entitled to recover damages that it could have avoided with reasonable efforts or expenditures. As to this defense, Orange must prove that: Telesocial failed to use reasonable efforts to mitigate its damages, and (2) the amount by which the damages could have been mitigated. *See Shaffer v. Debbas*, 17 Cal. App. 4th 33, 41 (1993). Here, Orange will be able to prove that Telesocial failed to use reasonable efforts to mitigate any of its damages.

Respectfully submitted,

ORANGE, S.A., et al.

By their attorneys,

/s/ Anthony D. Mirenda
Anthony D. Mirenda
FOLEY HOAG LLP

Dated: March 9, 2017

FILER'S ATTESTATION

Pursuant to Civil L.R. 5-1(i)(3), regarding signatures, I, Daralyn J. Durie, attest that concurrence in the filing of this document has been obtained.

/s/ Daralyn J. Durie
Daralyn J. Durie